รีวิว
ณัฐพล มงคลประดิษฐ์ สุรชัย เพิ่มสินทวี

NORTON ANTIVIRUS
ผู้พิชิตไวรัส

โปรแกรมป้องกันและ
ตรวจจับไวรัสที่เชื่อถือได้
จากปีเตอร์นอร์ตัน

ถ้าคุณเบื่อกับไวรัสพันธุ์ใหม่ ๆ ที่เล่นงานเครื่องคุณอยู่ผมขอแนะนำโปรแกรม Norton AntiVirus มาใช้งาน การใช้งานก็นับว่าง่ายมากคือจะมีพลูดาวน์เมนู และมี help คอยให้ความช่วยเหลือ หรือถ้าคุณต้องการปรับแต่งการทำงานเมื่อคุณโหลดโปรแกรม Norton AntiVirus เข้าเครื่องแล้ว คุณสามารถสั่งงานผ่าน Command-Line ได้ เช่น คุณอาจต้องการหรือไม่ต้องการให้มีเสียงเตือนเมื่อเจอไวรัส นอร์ตันแอนตี้ไวรัสจะฝังตัวไว้ในหน่วยความจำคอยตรวจสอบไฟล์และระบบที่คุณเรียกใช้งานว่ามีไวรัสหรือไม่ ที่สำคัญมันสามารถตรวจสอบไวรัสพันธุ์ใหม่ที่ยังไม่เป็นที่รู้จักได้ เปรียบเสมือนว่าคุณฉีดวัคซีนป้องกันไวรัสให้กับไฟล์ของคุณ นอกจากนี้ นอร์ตันแอนตี้ไวรัส ยังสามารถฆ่าไวรัสที่รู้จักออกจากไฟล์เมื่อตรวจพบได้

ความต้องการของระบบ

1. ทำงานบนเครื่องไมโครคอมพิวเตอร์ IBM-PC/XT/AT/PS-2 และเครื่องคอมแพตทิเบิ้ล

2. ใช้ได้ทั้งฟล็อบปี้ดิสก์ ฮาร์ดดิสก์ และอุปกรณ์เก็บข้อมูลทุกชนิดที่สามารถเคลื่อนย้ายได้

3. ใช้ระบบจัดการดอสรุ่นที่สูงกว่า 2.1

4. ต้องการหน่วยความจำแบบ RAM ขนาดตั้งแต่ 384 กิโลไบต์ขึ้นไป และใช้หน่วยความจำขนาด 24 กิโลไบต์ในการฝังตัว

5. ใช้งานร่วมกับเมาส์ได้

6. ใช้งานร่วมกับไมโครซอฟต์วินโดว์ได้

7. ใช้งานร่วมกับ networks หรือ LAN ได้ เช่น Novell และ IBM-Token Ring เป็นต้น

8. ไม่ป้องกันการก๊อบปี้

ไฟล์ต่าง ๆ ในนอร์ตันแอนตี้ไวรัส

INSTALL.EXE ใช้ในการติดตั้งโปรแกรมนอร์ตันแอนตี้ไวรัส

NAV.EXE เป็นโปรแกรมที่เรียกใช้ในการตรวจสอบไวรัส

NAV__.SYS ไดรเวอร์สำหรับป้องกันไวรัส

NAV.DEF ไฟล์ที่เก็บรายละเอียดของไวรัสพันธุ์ต่าง ๆ และเอาไว้ใช้ในการตรวจสอบและฆ่าไวรัส

NAV.HLP ไฟล์ที่คอยให้คำอธิบายส่วนต่าง ๆ ของการใช้งาน

NAV.ICO ไฟล์ที่นอร์ตันแอนตี้ไวรัสเอาไว้เรียกใช้ในไมโครซอฟต์วินโดว์

NAV.PIF ไฟล์ที่นอร์ตันแอนตี้ไวรัสเอาไว้เรียกใช้ในไมโครซอฟต์วินโดว์

UNINSTAL.EXE ใช้ถอดไฟล์ NAV__.SYS ออกจาก CONFIG.SYS

UNINSTAL.DOC ไฟล์ที่ใช้เก็บรายละเอียดของ UNINSTAL.EXE

UNINOC.EXE ใช้สำหรับลบ Checksum files ออก

UNINOC.DOC โปรแกรมเก็บรายละเอียดของ UNINOC.EXE

ฉีดวัคซีนป้องกันไวรัส

ในนอร์ตันแอนตี้ไวรัสจะทำการตรวจสอบไวรัสชนิดที่รู้จักและไวรัสชนิดที่ไม่รู้จักโดยการสร้างไฟล์เล็ก ๆ ที่เก็บลักษณะและขนาดที่แท้จริงของไฟล์ที่จะฉีดวัคซีน จะเรียกว่า checksum file ลักษณะไฟล์ที่ได้จะมีชื่อเหมือนไฟล์ที่จะฉีดวัคซีนแต่นามสกุลจะเปลี่ยนไปดังนี้

.COM คือ .__OM

.EXE คือ .__XE

.BIN คือ .__IN

.OVL คือ .__VL

.SYS คือ .__YS

checksum file จะมี attribute เป็นแบบ HIDDEN และ SYSTEM ซึ่งคุณจะมองไม่เห็นและลบไม่ได้ด้วยคำสั่งดอส ขนาดไฟล์จริงที่ใช้มีขนาดไม่เกิน 77 ไบต์ แต่โชคร้ายหน่อยตรงที่ขนาดไฟล์จะใหญ่ขึ้นเมื่อเก็บลงแผ่นดิสค์หรือถ้าเป็นฮาร์ดดิสค์จะมีขนาดระหว่าง 2 กิโลไบต์ ถึง 8 กิโลไบต์ เพราะดอสจะเก็บข้อมูลเป็นคลัสเตอร์ อย่างไรก็ตามผมคิดว่ามันก็คุ้มค่าต่อการเสี่ยงติดไวรัสที่จะมาทำลายระบบของคุณ แต่ถ้าคุณต้องการใช้เนื้อที่บนดิสค์สามารถลบได้ด้วยโปรแกรมเช่น PCTOOLS หรือใช้ไฟล์ UNINOC.EXE ที่มากับแผ่นก็ได้

นอร์ตันแอนตี้ไวรัสจะมีการแบ่งการทำงานออกเป็น 2 ส่วนดังนี้

1. Virus Intercept เป็นโปรแกรมประเภท Resident ที่ใช้ในการตรวจหาไวรัสในไฟล์ที่เรากำลังใช้งานอยู่ โดย Virus Intercept จะเป็นไฟล์ NAV__.SYS ที่เรานำไปใช้ในการบูตเครื่อง รายละเอียดขอให้ดูในเรื่องการติดตั้ง

2. Virus Clinic เป็นโปรแกรม NAV.EXE ที่เราเรียกใช้เพื่อทำการตรวจหาไวรัสและซ่อมไฟล์ที่ติดไวรัส

การติดตั้ง

การติดตั้งนอร์ตันแอนตี้ไวรัสในครั้งแรกนั้น เป็นเรื่องที่ค่อนข้างจะวุ่นวายเสียหน่อย แต่ผมจะขอสรุปวิธีการติดตั้งอย่างง่าย ๆ เอาไว้ก่อน หลังจากที่คุณได้อ่านและลองใช้ดูแล้วก็สามารถจะประยุกต์การติดตั้งใหม่ให้เหมาะสมกับการใช้งานของคุณเอง

1) ขั้นแรกต้องบูตเครื่องด้วยแผ่นดอสที่มั่นใจจริง ๆ ว่าไม่มีไวรัส จากนั้นก็นำเอาแผ่นดิสค์สำรอง หรือถ้าคุณมีฮาร์ดดิสค์ก็สร้างไดเรคทอรีย่อยขึ้นมาเพื่อทำการก๊อบปี้ไฟล์ทุกไฟล์มาจากแผ่นมาสเตอร์ หรืออาจเรียกใช้โปรแกรม INSTALL.EXE ก็ได้

2) เข้าไปในไดรฟ์หรือ PATH ที่คุณเพิ่งจะก๊อบปี้มา แล้วเรียกไฟล์ NAV.EXE โปรแกรมจะถามชื่อและบริษัทของคุณ และจะเก็บบันทึกเอาไว้ในไฟล์ NAV__.SYS หลังจากนั้นจอภาพก็จะปรากฏเมนู SCAN ขึ้นมา ให้กด "ESC" ออกจากเมนู SCAN เพื่อเข้าสู่เมนูหลัก

3) เข้าไปที่คำสั่ง OPTIONS พร้อมกับเลือกคำสั่ง CONFIGURATION ในพลูดาวน์เมนู ก็จะปรากฏ CONFIGURE ขึ้นมาให้เลือกดังรูปที่ 1 โดยมี CONFIGURE ที่สำคัญดังนี้

Remove Alert After [n] Seconds

ใช้ตั้งเวลาในการแสดงการเตือนของ Virus Intercept ขณะที่พบไวรัส หรือการเตือนอื่น ๆ คุณสามารถตั้งเวลาได้ไม่เกิน 59 วินาที และค่า Default ก็เป็น 59 วินาที

Alert Massage (a)

Configure นี้สามารถให้คุณแสดงข้อความของคุณเองได้ (ไม่เกิน 76 ตัวอักษร) ในขณะที่ Virus Intercept แสดงการเตือน โดยข้อความนี้จะอยู่ในวินโดว์ที่ใช้ในการเตือนด้วย โดย Alert Massage จะแสดงออกมาในกรณีต่าง ๆ ดังนี้

1) พบไวรัส

2) ในขณะที่หาไฟล์ Checksum File ไม่เจอ (ใน Advance Mode)

3) ไม่สามารถสร้างไฟล์ Audit Trail

Audit Trail (t)

Configure จะให้คุณใส่ชื่อไฟล์และ Path ของไฟล์ "Audit Trail" ซึ่งไฟล์นี้เป็นไฟล์ที่ใช้ในการบันทึกการเตือนของ Virus Intercept รวมทั้งวันที่และเวลาที่เตือนด้วย เพื่อคุณสามารถที่จะกลับมาอ่านบันทึกการเตือนได้

ถ้าเลือก Configure สองอันแรกแล้ว จำเป็นที่จะต้องใช้ไฟล์ Audit Trail โดยต้องใส่ชื่อไฟล์ Audit Trail และ Path ด้วย (มี Default เป็น B : \ AUDIT.LOG)

ส่วน CONFIGURE ต่าง ๆ ที่เหลือก็ให้คุณเลือกตามความเหมาะสมต่องานของคุณเอง หลังจากที่คุณเลือก CONFIGURE ทั้งหมดแล้ว ก็ให้กด <ENTER> จะทำได้ CONFIGURE ต่าง ๆ ถูกบันทึกไว้ในไฟล์ NAV__.SYS นอกจากนี้ภายในเมนู OPTIONS เราก็ยังสามารถตั้ง Pass Word เอาไว้เพื่อป้องกันการเปลี่ยนแปลง CONFIGURE ที่เราได้ตั้งเอาไว้ ซึ่ง Pass Word นี้จะใช้ได้ก็ต่อเมื่อเราทำการโหลด NAV__.SYS ในการบูตเรียบร้อยแล้ว ซึ่งจะกล่าวต่อไปในภายหลัง ส่วนเมนู Scan Option จะเป็นการเลือกโหมดของการ Scan ซึ่งแบ่งออกเป็น 2 โหมดดังนี้

Basic Mode จะเป็นการตรวจหาไวรัสที่นอร์ตันแอนตี้ไวรัสรู้จัก

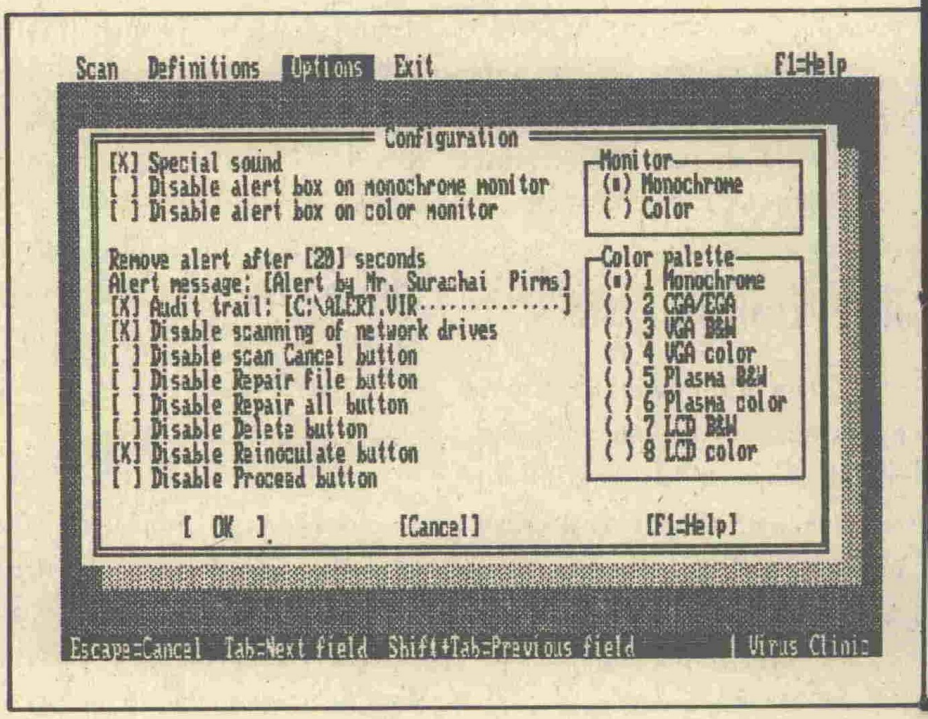
Advanced Mode จะเป็นการตรวจหาไวรัสทั้งที่นอร์ตันแอนตี้ไวรัสรู้จัก และไม่รู้จัก ส่วนการเซต Auto-Innoculate จะทำให้ Virus Intercept และ Virus Clinic สร้าง checksum file โดยอัตโนมัติ ถ้าไฟล์ที่จะรันนั้นไม่มี checksum file อยู่

4) หลังจากทำการเลือก OPTIONS ทั้งหมดแล้ว OPTIONS ทั้งหมดก็จะถูกบันทึกลงในไฟล์ NAV__.SYS ให้คุณก๊อบปี้ไฟล์ NAV__.SYS ไปยังแผ่นดอส และสร้างไฟล์ CONFIG.SYS ในแผ่นดอส ขึ้นมาใหม่โดยใส่คำสั่ง "DEVICE=NAV__.SYS" เพิ่มเติมเข้าไป ก็เป็นอันว่าสิ้นสุดขั้นตอนของการติดตั้ง

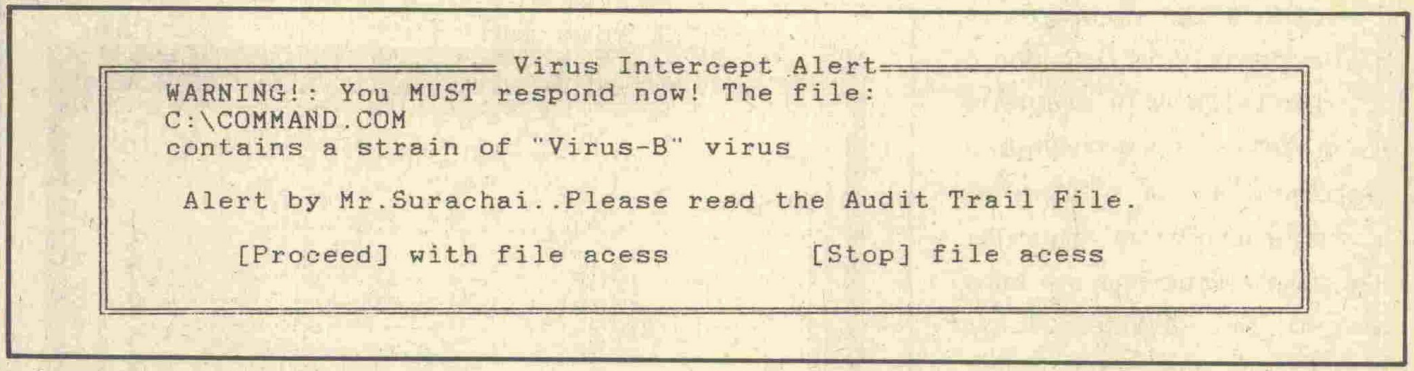
ถ้าคุณต้องการลบไฟล์ที่ติดไวรัสควรจะใช้โปรแกรม WIPEFILE.EXE ของ Norton Utilities หรือคำสั่ง Delete ใน Virus Clinic

การใช้งาน Virus Intercept

Virus Intercept ก็คือการตรวจหาไวรัสในขณะที่ไฟล์ต่าง ๆ กำลังถูกใช้งานอยู่ดังที่ได้กล่าวมาในตอนต้น โดยที่จริงแล้วก็คือ NAV__.SYS ที่ฝังตัวอยู่ในหน่วยความจำนั่นเอง ไฟล์ NAV__.SYS จะใช้เนื้อที่ฝังตัวอยู่ในหน่วยความจำประมาณ 24 กิโลไบต์ และจะทำการป้องกันตัวเองซึ่งเราจะไม่สามารถทำการอ่าน หรือเขียนไฟล์นี้ได้นอกจากจะติดต่อผ่านทางโปรแกรม NAV__.EXE เท่านั้น ในขณะที่ Virus Intercept ตรวจพบไวรัสก็จะแสดงข้อความเตือนออกมาดังรูปที่ 2 และถ้าคุณได้ติดตั้ง CONFIGURE ของ NAV__.SYS ให้สร้างไฟล์ "Audit Trail" ขึ้นมา คุณก็สามารถที่จะไปอ่านข้อความในไฟล์นี้ได้โดยใช้เวิร์ดโปรเซสเซอร์ หรือใช้คำสั่ง TYPE ในดอสก็ได้ จะเห็นข้อความที่ Virus Intercept ได้แสดงข้อความเตือนคุณว่าอะไรไปบ้าง พร้อมกับเวลา และวันที่



รูปที่ 1 เมนู Configuration



รูปที่ 2 แสดงข้อความเตือนของ Virus Intercept

การใช้งาน Virus Clinic

การใช้งาน Virus Clinic ให้เรียกไฟล์ NAV.EXE จะปรากฏเมนูคำสั่งให้เลือกโดยมีคำสั่งที่สำคัญดังนี้

Scan ใช้ในการตรวจหาไวรัสที่อยู่ทั้งในไดรฟ์ ไฟล์ และไดเรกทอรีต่าง ๆ ได้ดังในรูปที่ 3 โดยในโหมด Basic Scan จะตรวจหาไวรัสพันธุ์ได้ 142 ชนิด โดยในกรณีที่ไฟล์ของคุณติดไวรัสมากกว่า 1 ตัว นอร์ตันแอนตี้ไวรัสจะบอกเพียงไวรัสตัวสุดท้ายที่ตรวจพบเท่านั้น ดังนั้นคุณควรจะ Scan ไฟล์นั้นซ้ำอีกครั้งจนกว่าไม่เจอไวรัส

Definition จะเป็นการเพิ่มการตรวจจับไวรัสตัวใหม่ ๆ เข้าไป ซึ่งเราจะต้องนำเอาข้อมูลเกี่ยวกับไวรัสที่จะเพิ่มเข้าไป มาจาก Sysmantec's 24 hours Virus Newline ซึ่งเป็น BBS ของนอร์ตัน จึงจำเป็นที่จะต้องรอให้โปรแกรมมีการแพร่หลายของเมืองไทยเสียก่อน เช่นเดียวกับโปรแกรมประเภท SCAN.EXE, CLEAN.EXE เป็นต้น ซึ่งวิธีการเพิ่มไวรัสเข้าไปนั้นจะกล่าวถึงในตอนหลัง

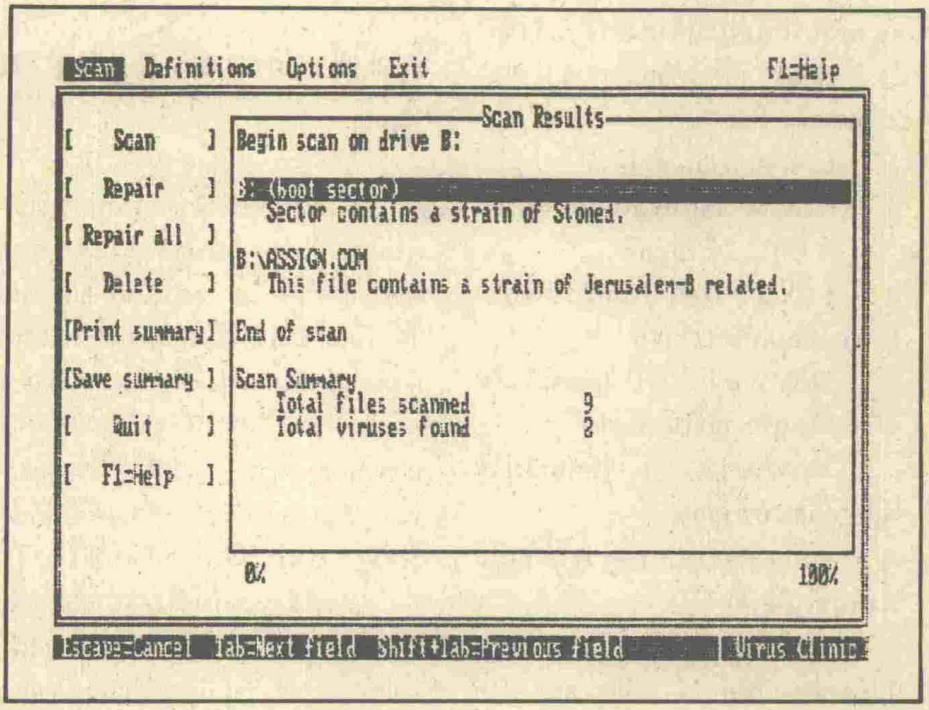
Options เป็นการตั้งค่า Option ต่าง ๆ ในการติดตั้งที่ได้กล่าวไปแล้ว

การเพิ่มชนิดของการตรวจจับไวรัส

การเพิ่มไวรัสเข้าไปในนอร์ตันแอนตี้ไวรัส คุณจะต้องมีข้อมูลเกี่ยวกับตัวไวรัสนั้น ๆ ซึ่งจะต้องนำเอามาจาก Bulletin Boards จากที่กล่าวไว้ข้างต้น หลังจากได้ข้อมูลมาแล้วก็ให้เข้ามาที่เมนู Definitions และ Add Virus Definition จะปรากฏวินโดว์ขึ้นมาดังรูปที่ 4 โดยแต่ละส่วนของวินโดว์จะเป็นดังนี้

NAME ให้ใส่ชื่อของไวรัสที่เราจะเพิ่มเข้าไป โดยจะตั้งชื่อให้เก๋ยังไงก็ได้ตามใจคุณ

LENGHT คือความยาวของข้อมูลไวรัสที่เราจะใส่

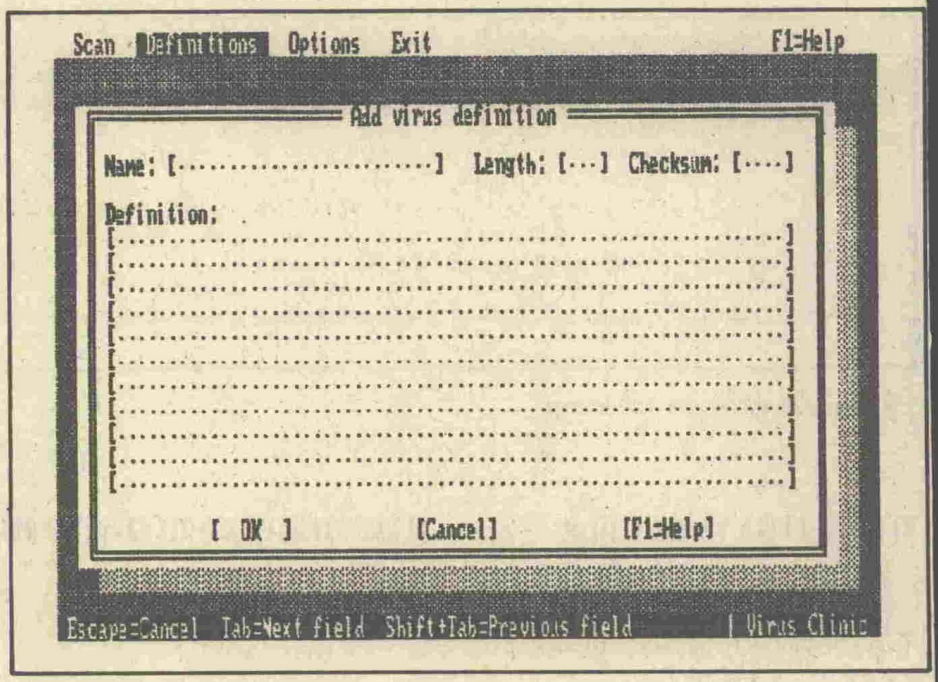


รูปที่ 3 หน้าต่างการตรวจหาไวรัส

CHECKSUM เป็นเลขฐาน 16 ที่ใช้ในการตรวจ Virus Definition

DEFINITION ให้ใส่ข้อมูลที่ได้มาจาก BBS โดยจะสามารถเขียนเป็นอักษรติดกันได้ทั้งหมด หรือเขียนที่ละ 4 ตัวอักษรและคั่นด้วย Space Bar ก็ได้ หลังจากเขียนเสร็จแล้วกด Enter เพื่อทำการ Save แล้วชื่อของไวรัสก็จะไปปรากฏขึ้นที่ List Virus Names

นอกจากนี้การเพิ่มชนิดไวรัสก็สามารถทำได้โดย การขอไฟล์ที่ทางนอร์ตันได้ทำเอาไว้แล้ว (มักจะมีนามสกุลเป็น *.DEF) มาเพิ่มเข้าไปโดยคำสั่ง Load Virus Definitiions ในเมนู DEFINITIONS



รูปที่ 4 หน้าต่างการเพิ่มไวรัส

การใช้งานนอร์ตันแอนตี้ไวรัสแบบ Command-Line

คุณสามารถเรียกใช้งาน NAV.EXE แบบ Command-Line โดยไม่ต้องเข้าไปในเมนู มีคำสั่งต่าง ๆ ดังนี้

NAV/? แสดงตัวเลือกต่าง ๆ แบบ command line

NAV/A scan ทุกไดรฟ์

NAV/M ใช้กับจอโมโนโครม

NAV/C ใช้กับจอสี

NAV/S {+/−} ใช้และไม่ใช้เสียงในการเตือนเมื่อพบไวรัส

NAV / 0 {+/−} ใช้และไม่ใช้บล็อกเตือนหน้าจอโมโนโครม

NAV/X {+/−} ใช้และไม่ใช้บล็อกเตือนหน้าจอสี

NAV/ {DRIVE:} ตรวจสอบไฟล์ทั้งหมดในไดรฟ์

NAV/ {Filename} ตรวจสอบไวรัสเฉพาะไฟล์ ใช้ Wild card หรือ * ? ได้

คุณสามารถใช้พารามิเตอร์หลายอันร่วมกันได้โดยให้เว้นวรรคแต่ละพารามิเตอร์ไว้ เช่น NAV/C+/M

การใช้งานร่วมกับโปรแกรมอื่น ๆ

นอร์ตันแอนตี้ไวรัสจะไม่สามารถตรวจสอบโปรแกรมที่เกิน 640 กิโลไบต์ หรืออยู่เหนือ conventional memory ได้ เมื่อต้องการใช้โปรแกรมประเภทที่ฝังตัวอยู่เหนือ conventional memory ควรจะ scan ไฟล์นั้นก่อนเรียกใช้ และควรโหลด NAV__.SYS ไว้ใน conventional memory ด้วยเพื่อให้ไฟล์ NAV__.EXE สามารถเรียกใช้ได้

การใช้งานร่วมกับ QEMM หรือ 386Max เป็นโปรแกรมที่จัดการเกี่ยวกับหน่วยความจำ จะมีการเรียกใช้ video RAM หรือ หน่วยความจำที่ตำแหน่ง (B000-B7FF) ซึ่งจะซ้ำกับการเรียกใช้ของนอร์ตันแอนตี้ไวรัส ดังนั้นคุณต้องไปกำหนดให้ QEMM หรือ 386Max ไม่ให้เรียกใช้หน่วยความจำส่วนนี้โดยเข้าไปแก้ใน CONFIG.SYS ดังนี้

device=qemm.sys x=b000-b7ff สำหรับโปรแกรม QEMM

device=386max.sys x=b000-b7ff สำหรับโปรแกรม 386Max

การใช้งานร่วมกับ DesqView เป็นโปรแกรมที่ช่วยในการเปิดไฟล์ได้หลายไฟล์พร้อมกันหรือเรียกว่า multi-tasking DesqView มีความสามารถในการใช้ระบบก่อนโปรแกรมอื่น ทำให้การเตือนเมื่อเจอไวรัสของนอร์ตันแอนตี้ไวรัสไม่สามารถหยุดระบบทั้งหมดได้ อาจทำให้การป้องกันของนอร์ตันแอนตี้ไวรัสไม่ได้ผล วิธีที่ป้องกันความเสียหายให้เกิดน้อยที่สุดคือคุณต้องสังเกตและตอบรับการเตือนของนอร์ตันแอนตี้ไวรัสให้เร็วที่สุด

นอร์ตันแอนตี้ไวรัสไม่ compatible กับ Double-DOS Referee multitaskers และ TSR managers อื่น ๆ เพราะเกิดการขัดแย้งในการเรียกใช้ DOS Interrupt

การใช้งานร่วมกับโปรแกรม back-up คุณควรกำหนด scan options ใน Virus Clinic เป็น Basic Mode มิฉะนั้นนอร์ตันแอนตี้ไวรัสจะเตือนคุณตลอดเวลาเมื่อคุณ backup ไฟล์ที่ยังไม่ได้ฉีดวัคซีน หรือคุณอาจจะบูตเครื่องใหม่โดยไม่โหลด NAV__.SYS ได้ด้วยการกดปุ่ม Shift keys ทั้งสองข้างพร้อมกันหลังจากได้ยินเสียง "บี๊บ" ขณะเครื่องกำลังบูต

การใช้งานร่วมกับ Attach Mate เป็นโปรแกรมประเภท TSR ที่ช่วยให้ไมโครคอมพิวเตอร์ติดต่อกับ mainframe ได้ คุณควรเพิ่มบรรทัด

set acpint=61

ลงใน AUTOEXEC.BAT มิฉะนั้นจะทำให้ระบบหยุดทำงานหรือหยุดทำงานเมื่อคุณกด <Crtl> <Alt> k ได้

เมื่อใช้กับ LAN หรือ Network คุณควรกำหนดให้ Scan Options เป็นแบบ Basic mode หรือเป็นแบบ Avanced mode และยกเลิก Auto-Inoculate เพื่อป้องกันไม่ให้สร้าง check-sum file แต่ถ้า Network ที่คุณใช้มีการฉีดวัคซีนไว้คุณสามารถตั้ง Scan Options เป็น Advanced mode แบบมี Auto-Inoculate ได้

การใช้งานร่วมกับไมโครซอฟต์วินโดว์คุณควรปรับ "Remove alert after__seconds" ใน Option menu ให้มีเวลาอย่างต่ำ 1 วินาที และปรับให้มีการเตือนของ Alert boxes เพราะว่า Auto-inoculate จะไม่สร้าง check-sum file ให้กับ .SYS ไฟล์ ทำให้เมื่อไมโครซอฟต์วินโดว์ถูกโหลดเข้ามา Virus Intercept จะมีข้อความเตือนให้คุณฉีดวัคซีนไฟล์ .SYS ของไมโครซอฟต์วินโดว์และถ้าคุณยกเลิกการเตือนของ Virus Intercept ไมโครซอฟต์วินโดว์จะไม่ทำงาน เพื่อหลีกเลี่ยงปัญหานี้คุณควรสร้าง Batch file ดังนี้

NAV/S+/O-/X-
WIN
NAV/S+/O+/X+

บรรทัดแรกกำหนดให้ Virus Intercept สร้างเสียงในการเตือนแทนการเตือนด้วยข้อความ

บรรทัดที่สอง เรียกใช้งานโปรแกรมไมโครซอฟต์วินโดว์

บรรทัดที่สาม ปรับให้มีการเตือนบนจอภาพดังเดิม

ข้อควรระวัง

เวลาใช้งานกับเครื่องพิมพ์ คุณควรที่จะ on-line เครื่องพิมพ์ และใส่กระดาษไว้ให้เรียบร้อย มิฉะนั้นเครื่องคอมพิวเตอร์อาจเกิดอาการ hang ขณะที่นอร์ตันแอนตี้ไวรัสรอข้อความจากดอส เมื่อเกิดข้อผิดพลาดจากเครื่องพิมพ์

ข้อจำกัดของ Virus Intercept

Virus Intercept จะไม่ป้องกันระบบในการติดไวรัส เมื่อคุณก็อบปี้โดยใช้คำสั่ง DISKCOPY ในดอส หรือใช้โปรแกรม Disk Editor หรือ NU.EXE ทำให้ไวรัสอาจจะก็อบปี้ไปในโปรแกรมได้

Virus Intercept ไม่สามารถตรวจสอบโปรแกรมที่ compress หรือโปรแกรมที่ใส่รหัสเอาไว้เพื่อป้องกันการใช้ คุณควรที่จะ decompress หรือถอดรหัสไฟล์ออกก่อนแล้วจึงจะตรวจสอบได้

การป้องกันตัวเองของ Virus Intercept

เมื่อ NAV__.SYS โหลดเข้าไปในหน่วยความจำแล้ว Virus Intercept จะป้องกันตัวในการอ่านและเขียนจากโปรแกรมอื่น คุณจึงไม่สามารถ view, erase, modify หรือเปลี่ยน attribute ของไฟล์ NAV__.SYS ได้ทำให้เวลาคุณใช้โปรแกรม File Find หาไฟล์ NAV__.SYS หรือ NAV__.* จะปรากฏออกมาทุกแห่ง และในการ backup คุณไม่ควรรวมไฟล์ NAV__.SYS ไปด้วย

สรุป

จากเรื่องราวของนอร์ตันแอนตี้ไวรัสที่ได้กล่าวมานี้ คุณอาจจะคิดว่ายังไม่จำเป็นที่จะต้องใช้มัน เพราะใช้เนื้อที่บนดิสก์ในการตรวจสอบไวรัส แต่นอร์ตันแอนตี้ไวรัสมีข้อได้เปรียบในเรื่องการตรวจหาไวรัสที่ไม่รู้จักได้ดังที่กล่าวมาแล้ว และยังสามารถเพิ่มประสิทธิภาพในการตรวจหาไวรัสได้ตลอดเวลา โดยไม่ต้องรอการเปลี่ยนรุ่นของโปรแกรม

ผู้เขียนหวังว่าเมื่อโปรแกรมนี้แพร่หลายออกไปแล้ว อาจจะมีผู้อ่านบางท่านสามารถหาข้อมูลไวรัสตัวใหม่ ๆ มาเพิ่มในโปรแกรมได้ ก็ขอให้นำมาเผยแพร่ต่อไปในเมืองไทยต่อไปเช่นเดียวกันกับโปรแกรมตรวจหาไวรัสตัวอื่น ๆ สำหรับผู้ที่สนใจโปรแกรมนี้ลองหาดูได้ที่ร้านบุ๊คเซลล์ สยามสแควร์ซอย 2 ได้ครับ